HSE Ireland Incident Response Policy

[HSE-IR-POL-2024]

Prepared by: Gaurav Suryawanshi
as a part of
CYBERSEC 510.02. Fa24

Document Control Section	
Document Title	Incident Response Policy
Document Number / Internal Code Reference	HSE-IR-POL-2024
Classification	TLP: AMBER (Limited Disclosure)
Location	HSE Master -> SOP Files OneDrive

Authorization		
Document Owner	**Reviewed By**	**Approved By**
ITIS, IS Steering Committee, IRT (co-owner)	Gaurav Suryawanshi (self)	Gaurav Suryawanshi (self)

Review/Amendment/Changelog				
Version	**Modification Date**	**Section**	**A/M/D**	**Brief Description of Change/Review (performed by – details)**
v0.1	18th October, 2024	1-6	n/a	Policy creation

Table of Contents

1. INTRODUCTION

1.1 PURPOSE

Incident response capabilities are essential for monitoring security incidents, assessing their severity and taking appropriate action. Without such capabilities, security incidents may go unnoticed, leading to greater potential harm compared to when they are promptly identified and addressed.

HSE is dedicated to safeguarding the privacy and security of its confidential as well as non-confidential data. In the event of a potential breach of this sensitive information, HSE will conduct a thorough investigation into the suspected breach and implement suitable corrective and remedial measures.

1.2 OBJECTIVE

The main objectives of incident response include identifying the causes and effects of incidents, determining appropriate sanctions, implementing preventive measures, and restoring affected infrastructure promptly.

HSE acknowledges that all incidents are also considered information security events. However, not all events lead to incidents. An event is reported whenever something unusual occurs, whether planned or unplanned, without causing a service or system interruption or any other compromise that would be classified as an incident.

This Incident Response Policy and its accompanying addenda aim to establish an incident response program with the authority to form an incident response team and set standardized procedures for addressing security-related events affecting HSE's information technology resources. A standardized approach to managing security-related events will enable comprehensive information gathering and reporting, as well as timely remediation.

Information is a crucial asset of the company and accurate, timely, relevant, and properly protected information is vital to the company's operations. To ensure proper handling of information, all access to, and use and processing of, HSE’s information must be in line with HSE Information Systems related policies and standards.

1.3 APPLICABILITY

This Incident Response Policy is applicable to all individuals utilizing any information resources related to HSE.

1.4 SCOPE

This policy encompasses all information systems, data, information system components, and users of HSE’s information technology resources, governing the company’s general response, documentation, and reporting of security incidents affecting those resources.

This includes but is not strictly limited to:

- Servers and other devices that provide centralized computing capabilities
- Devices or applications that provide storage capabilities
- Desktops, laptops, and other devices such as smartphones and tablets, that provide distributed computing
- Routers, switches, and other devices that provide network capabilities
- Firewalls, IDS sensors and other devices that provide dedicated security capabilities
- Databases and files contained in above systems
- Restricted and Confidential data contained in the above systems
- Restricted and Confidential information, paper-based

2. POLICY

HSE defines an Information Security Incident as any activity that harms, compromises, or threatens to harm or compromise HSE's information technology resources or restricted and sensitive information. This includes acts or omissions causing service interruption, inhibition of functioning systems, unauthorized changes to hardware, firmware, software, or data, and unauthorized exposure, change, deletion, or destruction of information. Although efforts have been made to align this policy with the state of technology at its adoption date, technological advancements may surpass certain aspects of this policy. Therefore, employees are expected to be sensitive to the underlying spirit and intent of this policy and should not attempt to circumvent its goals indirectly. Violations of this policy must be reported immediately to the ITIS, IRT or the IS Steering Committee for timely documentation, investigation, containment, and remediation of the security event or incident.

3. RESPONSIBLE PARTIES

The Incident Commander (IC) is responsible for establishing an Incident Response Team (IRT) to respond to incidents, including intervention, remediation, and security-related investigations. Core members are selected for the team based on their job functions within HSE, and specific department representatives may be required based on the type and severity of the incident. The Incident Response Team is responsible for determining the involvement trigger points for other HSE business units and functional departments and involving applicable groups based on specific requirements outlined by those groups.

This following plan governs all types of security incidents -

A.16.1 Management of information security incidents and improvements	
Control Statements	**ISO 27001** **Annex A Reference**
HSE has established clear responsibilities and procedures to ensure prompt review of events and to facilitate a swift and organized response to any information security incidents.	A.16.1.1 Responsibilities and procedures
It is the policy of HSE that any information security events should be promptly reported through the appropriate management channels in accordance with the representatives listed above. If an HSE employee witnesses or becomes aware of an event and is unsure about the management representation, they should immediately reach out to the IS Steering Committee or People Ops to report the event.	A.16.1.2 Reporting of security incidents
Employees, contractors, or vendors of the HSE's departments are encouraged to report any incidents, events, activities, or concerns to a member of the IS Steering Committee. Additionally, the Business Technology & Information Services team may detect incidents through proactive monitoring of HSE's information technology resources. Upon reporting, the matter will be referred to the Incident Response Team for assessment and necessary action.	A.16.1.3 Reporting information security weaknesses

4. PROCEDURE

4.1 IDENTIFICATION AND CLASSIFICATION

The classification of the type of security incident and its severity should be determined based on the most accurate information available at the time and adjusted as new information emerges.

4.1.1 Type of Event

Security events can manifest in various forms, including but not limited to:

- A phishing campaign for password resets
- A phishing campaign targeting direct deposit changes
- A phishing campaign targeting fraudulent wire transfers
- A violation of security policies
- A breach of information
- Attempts to gain unauthorized access
- Excessive port scans
- A denial-of-service attack
- Malicious code outbreak
- Unauthorized use or modification of resources
- Defamation of brand (hacking and/or defacing HSE's website or social media accounts)
- Civil unrest
- Theft

After a thorough investigation has been conducted, an Event may be escalated to an Incident if it meets the specific criteria outlined in Section 2 of the policy.

4.1.2 Threat level of an Incident

Upon categorization of an event as an incident, the Incident Response Team is tasked with establishing an incident classification matrix to effectively tailor the response and engage the relevant team members. This matrix serves to prioritize the incident and determines the involvement of HSE teams, stakeholders and applicable procedures for each incident class.

Critical assessment of an incident is essential for determining the involvement of individuals, including relevant law enforcement authorities such as local police or the FBI, and evaluating the severity of the incident. In certain cases, the ranking may be adjusted based on the potential damage to HSE and its affiliates, irrespective of meeting the specified criteria.

Information security incidents, including but not limited to cyber-security incidents, will be rated per the following severities:

Severity	Description
Critical	Critical exposure refers to a significant release of information, assets, or services that severely impacts HSE internally as well as externally through reputation and/or monetary damages, along with the systems at scale. In severe cases, critical rankings are assigned, requiring the involvement of multiple members within the organization. Such critical rankings may be escalated to the relevant law enforcement authorities as outlined in the proposed Business Continuity Plan (HSE-BCP-PLN-2024-draft) for HSE. Executive team members are to be involved in managing critical incidents.
High	An incident is classified as any event that has a detrimental effect on business operations or compromises the confidentiality, integrity, or availability of systems. Higher classifications may include targeted attacks or widespread virus outbreaks. Incidents with high rankings may be reported to the relevant law enforcement authorities as outlined in the HSE's proposed Business Continuity Plan (HSE-BCP-PLN-2024-draft). Executive team members may be involved in handling high-priority incidents.
Medium	Instances demanding prompt action to address a specific threat that does not directly result in significant harm to the organization but has the potential to escalate if not addressed. Incidents with medium severity may be reported to the relevant law enforcement agencies as outlined in the HSE's proposed Business Continuity Plan (HSE-BCP-PLN-2024-draft)
Low	Incidents that do not result in damage to HSE's assets necessitate thorough investigation to ensure that the incident is managed appropriately. Incidents with low severity ratings are unlikely to be further escalated.

4.2 IMMEDIATE TRIAGE AND RESPONSE

Upon receipt of a report regarding an event, activity, or concern, the Incident Commander or the Incident Response Team will promptly assess its validity to ascertain whether it qualifies as an Incident. If confirmed as an Incident, the designated official will categorize it and assign a priority classification.

HSE models the IR lifecycle based on NIST SP 800-61 guidance which divides the process into four phases.

4.3 INCIDENT RESPONSE STEPS

4.3.1 Key Phases

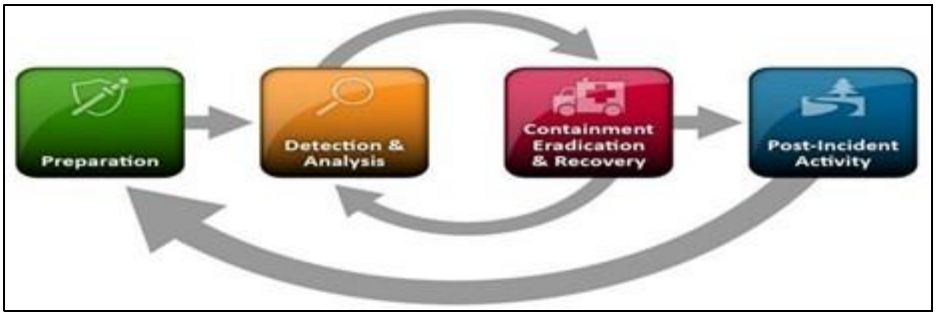

Figure 4.1 IR phases during a breach/incident response

Preparation

Measures implemented to minimize the likelihood of a security incident and to ensure that the organization is well-prepared to defend itself.

Detection & Analysis

Efforts to identify potential security incidents and understand their impact on the organization, as well as activities aimed at maintaining awareness of various threats.

Containment, Eradication & Recovery

Proactive steps taken to minimize the impact of a confirmed security incident and restore the environment to a secure state.

Post-Incident Activity

Conducting after-action reviews to gather insights and enhance the organization’s incident response capabilities.

4.3.2 Detection

The most challenging aspect of this procedure is identifying a security incident among the regular daily activity. Reports of an event can originate from various sources, including employees, vendors, customers, partners, or facility management. The Incident Commander evaluates the information to determine if an incident has occurred and then moves on to the assessment phase, bringing in additional team members as necessary.

4.3.3 Analysis

A.16.1 Management of information security incidents and improvements	
Control Statements	**ISO 27001** **Annex A Reference**
Upon evaluation, not all reported incidents are categorized as information security incidents. The Incident Response Team, in conjunction with the affected business area, will conduct an assessment to determine and classify relevant events as information security incidents.	A.16.1.4 Assessment of and decision on information security events

When an event meets the criteria of an incident, the Incident Response Team must follow a formal and systematic process to respond to the incident. This process consists of several phases, starting from initial response preparation and ending with post-incident analysis.

The Incident Response Team will collaborate with others as necessary and take the appropriate steps to investigate, gather evidence, analyze, contain, eradicate, and remediate the incident. The team is responsible for documenting the entire incident response process. The Incident Response Team must assess the impact and magnitude of the incident. It's crucial not to rush into action, such as turning off a computer, as this could result in data loss, or the destruction of evidence needed for a later investigation. Factors to consider include:

- How many computers are affected?
- Is secret information involved?
- What is the entry point of the incident?
- What is the potential damage?

- What is the estimated recovery time?
- What external agencies (e.g., law enforcement authorities, clients) need to be notified?
- What additional resources may be required?
- Was any customer data compromised?

As determined by the Incident Response Team's evaluation, appropriate notifications will be sent to senior management, customers, law enforcement authorities, and any affected vendors or services. In the event of a breach of customer Personally Identifiable Information (PII), all legal requirements for breach notification will be strictly followed. If a breach involving customer PII occurs, the affected customers will be informed with the aim of establishing a coordinated response.

4.3.4 Containment

A.16.1 Management of information security incidents and improvements	
Control Statements	**Annex A Reference**
HSE involves responding to incidents based on the type of information security incident. The Incident Response Team is responsible for determining whether the incident should be escalated internally to the Cybersecurity Leadership Team or externally to law enforcement authorities before responding, as well as deciding on the appropriate response method.	A.16.1.5 Response to information security incidents

To regain control and minimize harm, the Incident Response Team may decide to isolate the compromised system from the rest of the network. However, careful consideration must be given to the potential impact this action may have on the business operations. Additionally, the Incident Response Team may decide to change passwords to thwart the installation of Trojan programs that could create unauthorized access points. For non-IT incidents, containment measures may involve engaging law enforcement authorities, replacing assets, and/or providing education to employees.

4.3.5 Eradication and Recovery

Once an event has been classified as an incident, it is important to conduct a thorough investigation to determine the root cause. This may involve reviewing logs from multiple systems. Caution should be exercised when using administrative tools on the compromised system, as they may have also been compromised to cause further damage. Consider using a separate set of administrative tools.

Following the investigation, a clean operating system should be installed and fortified with the latest patches. This includes disabling unnecessary services, installing anti-virus software, and implementing any additional security requirements as per the policy. Once business operations are restored, the system should undergo testing in a controlled environment before being reintroduced into production. Additional monitoring measures should be implemented in the production environment to detect any potential return by the attacker.

4.3.6 Post-Incident Activity

A.16.1 Management of information security incidents and improvements	
Control Statements	**ISO 27001** **Annex A Reference**
After addressing and resolving a particular incident, a review will be conducted to document the effectiveness of the current incident response program and the handling of the specific event. Preventive measures will also be identified to prevent a recurrence of the same incident.	A.16.1.6 Learning from information security incidents

The Incident Response Team will conduct a thorough analysis to ascertain the cause of the incident and identify preventive measures. Additionally, if legal action is necessary, external investigators may be needed to preserve the integrity of evidence for admissibility in court.

A.16.1 Management of information security incidents and improvements	
Control Statements	**ISO 27001** **Annex A Reference**
HSE has implemented measures to ensure that evidentiary records are clearly defined. Procedures have been established for the identification, collection, acquisition, and preservation of any information that could serve as evidence. The Incident Response Team is responsible for ensuring that all events and incidents are properly logged and archived. Representatives of the Incident Response Team are tasked with promptly communicating incidents to the relevant personnel and maintaining contact for updates and instructions throughout the incident. A summary report on information security incidents will be provided to the Executive Governance and IS Steering Committees on a monthly basis. The Incident Response Team will utilize standard internal procedures to log and track incidents and will be responsible for maintaining these records.	A.16.1.7 Collection of evidence

The necessary documentation should be appropriately attached to the incident ticket. In addition to a summary tailored for managerial review, the documentation may encompass:

- System events with audit records
- Actions taken including the time performed
- Notes from external conversations including person, time, and content

- A description of the exact sequence of events
- Method of discovery
- Preventative measures added
- Further recommendations

The primary objective of documentation is to enhance the efficacy of systems and procedures, which encompasses the incident response approach.

4.3.7 Prevention

HSE's IRT consistently monitors and scans its network to prevent events and subsequent incidents. It also continues to develop clear protection procedures for the configuration of its Information Technology Resources. The Incident Response Team is responsible for properly recording incidents in its system of records. After the closure of an incident, the security team conducts a post-incident review to capture lessons learned and track identified areas of improvement.

4.4 SUSPICIOUS ACTIVITY NOTIFICATION

It is imperative that an individual reports any observed suspicious activity to the security team via email at security-IRT@HSE.ie and Business Technology & Information Services at BTIS@HSE.ie

The Incident Response Team will undertake a comprehensive review of any potential incidents. In the case of potentially critical incidents, the Incident Response Team will expeditiously alert the IS Steering Committee and the Cybersecurity Leadership Team as necessary.

In confirmed data breach incidents involving sensitive customer data, the Incident Response Team will collaborate with the Cybersecurity Leadership Team to promptly notify the respective customer's security team within 24 hours of confirmation, and with Executive approval.

5. COMPLIANCE

It is crucial for the business success of HSE and the information security management program that all employees comply with this policy. As an employee of HSE, it is your responsibility to:

- Learn and understand the requirements of this policy
- Apply the requirements of this policy to your job responsibilities and activities
- Comply with the outlined requirements of this policy as detailed in Section 2
- Fully cooperate in any audit or investigation related to any suspected event or violation of this policy
- Report any violation of this policy to the IS Steering Committee

If you are a manager or supervisor, you have additional responsibilities, including:

- Ensuring that associates know and understand this policy and its appropriate application
- Taking proactive steps to prevent violations of this policy
- Establishing proactive methods to identify if violations of this policy have occurred
- Ensuring that any associate who reports a suspected violation of this policy is protected from retaliation

6 DISCIPLINARY ACTIONS

Violation of this policy may lead to disciplinary measures, including termination, for employees, including temporary staff. Please consult the internal HSE's Disciplinary Policy (HSE-ISEC-D-POL-1) specific to each location for further details.

6.1 EXCEPTIONS

This policy covers cybersecurity requirements associated with incidents and breaches in HSE's assets and environments. Even with the most comprehensive policies and procedures in place, it is important to understand and accept that there might be situations where exceptions and limitations apply.

These exceptions can stem from technical constraints, business decisions or other unforeseen circumstances. However, by outlining and acknowledging them HSE ensures transparency and an understanding of the broader risk landscape. HSE would grant exception of this policy only

a.) In the case of justified business requisites with approval from IS Steering Committee / CISO

b.) The minimum-security requirements are met in low-risk cases without affecting actual business requirements and where security risks are mitigated by detective, deterrent and/or compensating controls.

Exceptions shall be formally submitted to the IS Steering Committee including justifications and benefits attributed to the exception. The policy waiver period will be valid for one year and shall be reassessed and reapproved, if necessary for a maximum of three consecutive terms. No policy shall be provided an exception for more than three consecutive terms.

6.2 ESCALATION MATRIX / CONTACT INFORMATION

Escalation Level	Department / Role	Email	Response Time SLA
L1 (Level 1)	Incident Response Team (IRT)	security-IRT@HSE.ie	15 minutes
L2 (Level 2)	Incident Commander	security-IC@HSE.ie	30 minutes
L3 (Level 3)	Security Operations Manager	SOC24x7@HSE.ie	1 hour
L4 (Level 4)	Chief Information Security Officer (CISO)	CISO@HSE.ie	2 hours
L5 (Level 5)	Legal Counsel	Ext-LegalCounsel@HSE.ie Legal@HSE.ie	4 hours

6.3 RACI MATRIX

Responsible (R)	Accountable for executing the work	Incident Response Team
Accountable (A)	Responsible for making the final decision	Incident Commander
Consulted (C)	Required to be consulted before taking any action or making a decision (proactive)	IS Steering Committee

Informed (I)	Informed after a decision or action has been taken (reactive)	Cybersecurity Leadership Team Other parties affected by the change

Appendix A: Glossary and Definitions

ITIS	Information Technology and Information Security
IRT	Incident Response Team
IC	Incident Commander
A/M/D	Added, Modified, Deleted
IS Steering Committee	Information Security Steering Committee
SOC	Security Operations Center
CISO	Chief Information Security Officer
Personnel	Group of people affiliated as HSE employees, temporary staff, sub-contractors, contractors, interns

Appendix B: Linkage to other relevant documents

The policy uses terms, abbreviations and cross-references which are liaised in the [HSE-IR-PLN-2024] and [HSE-PLYBK-001] documents. Following are the attached copies of the documents prepared by the consultant.

[HSE-IR-PLN-2024]	PDF HSE Incident Response Plan v0.1.pc
[HSE-PLYBK-001]	PDF HSE Ransomware Playbook v0.1.pdf